We claim:

1. A method of forward enhanced CMEA encryption or decryption cryptoprocessing for each message in a call, for use in a CMEA encryption system employed in a wireless telephone system comprising the steps of:

introducing an unprocessed message or encrypted message;

creating one or more secret offsets;

performing a first transformation on the unprocessed message to produce a first transformed message;

performing an iteration of the CMEA process on the first transformed message to produce an intermediate ciphertext message, the iteration of the CMEA process employing an enhanced tbox function using an involutary lookup, the inputs to the enhanced tbox function being subjected to a permutation using one or more of the secret offsets to produce a permutation result; and

performing a second transformation on the intermediate ciphertext message to produce a final processed message;

2. The method of claim 1 wherein the one or more secret offsets include a first and a second secret offset.

3. The method of claim 2 wherein the step of generating each of the first and second offsets includes combining ones of a plurality of secret values with a an external value.

4. The method of claim 3 wherein the secret values include two 8-bit values for each offset.

5. The method of claim 4 wherein the external value is an 8-bit value.

6. The method of claim 5 wherein the first offset for an nth message of a call is expressed by the equation offset1 = $((K_0 + 1) * CS_n \bmod 257) \oplus K_1 \bmod 256$, where K_0 and K_1 are ones of the secret values and CS_n is an external value for the nth message, and wherein the

second offset for an nth message of a call is expressed by the equation offset2 = $((K_2 + 1) * CS_n \bmod 257) \oplus K_3 \bmod 256$, where K_2 and K_3 are ones of the secret values and CS_n is an external value for the nth message.

7. The method of claim 6 wherein the first transformation includes performing the steps of bit trading, involutary lookup with feedback, and random byte permutation on each octet of the unprocessed message, wherein the steps of bit trading and random byte permutation each employ the first secret offset, and wherein the step of involutary lookup with feedback employs both the first and second secret offsets.

8. The method of claim 7 wherein the second transformation includes the steps of bit trading, involutary lookup with feedback, and random byte permutation on each octet of the intermediate ciphertext message, wherein the steps of bit trading and random byte permutation each employ the second secret offset, and wherein the step of involutary lookup with feedback employs both the first and second secret offsets.

9. A method of reverse enhanced CMEA cryptoprocessing for each message in a call, for use in a CMEA encryption system employed in a wireless telephone system, comprising the steps of:

introducing an unprocessed message or encrypted message;

creating one or more secret offsets;

performing a first inverse transformation on the unprocessed message to produce a first inverse transformed message;

performing an iteration of the CMEA process on the first inverse transformed message to produce an intermediate ciphertext message, the iteration of the CMEA process employing an enhanced tbox function using an involutary lookup, the inputs to the enhanced tbox function being subjected to a permutation using one or more of the secret offsets to produce a permutation result; and

performing a second inverse transformation on the intermediate ciphertext message to produce a final processed message;

10. The method of claim 9 wherein the one or more secret offsets include a first and a second secret offset.

11. The method of claim 2 wherein the step of generating each of the first and second offsets includes combining ones of a plurality of secret values with an external value.

12. The method of claim 11 wherein the secret values include two 8-bit values for each offset.

13. The method of claim 12 wherein the external value is an 8-bit value.

14. The method of claim 5 wherein the first offset for an nth message of a call is expressed by the equation offset1 = $((K_0 + 1) * CS_n \bmod 257) \oplus K_1 \bmod 256$, where K_0 and K_1 are ones of the secret values and CS_n is an 8-bit external value for the nth message, and wherein the second offset for an nth message of a call is expressed by the equation offset2 = $((K_2 + 1) * CS \bmod 257) \oplus K_3 \bmod 256$, where K_2 and K_3 are ones of the secret values and CS_n is an 8-bt external value for the nth message

15. The method of claim 14 wherein the first inverse transformation includes the steps of performing random byte permutation, involutary lookup with feedback, and bit trading on each octet of the unprocessed message, wherein the steps of bit trading and random byte permutation each employ the second secret offset, and wherein the step of involutary lookup with feedback employs both the first and second secret offsets.

16. The method of claim 15 wherein the second inverse transformation includes the steps of performing random byte permutation, involutary lookup with feedback, and bit trading on each

octet of the intermediate ciphertext message, wherein the steps of bit trading and random byte permutation each employ the first secret offset, and wherein the step of involutary lookup with feedback employs both the first and second secret offsets.

17. A wireless handset for securely transmitting messages, comprising:

a transceiver;

an input/output interface;

a key generator for generating one or more keys to be used during a call; and

a cryptoprocessor for receiving from the input/output interface a message to be encrypted or decrypted together with identification of the message as plaintext to be encrypted or ciphertext to be decrypted and processing the message as using a forward enhanced CMEA process including first and second transformations and a CMEA iteration including an ehanced tbox function with inputs permuted by one or more secret offsets, the enhanced tbox function employing an involutary lookup table, the encryption/decryption processor being further operative to return the encrypted or decrypted message to the input/output interface for further routing.

18. A wireless base station for securely transmitting messages, comprising:

a transceiver;

an input/output interface;

a key generator for generating one or more keys to be used during a call; and

a cryptoprocessor for receiving from the input/output interface a message to be encrypted or decrypted together with identification of the message as plaintext to be encrypted or ciphertext to be decrypted and processing the message as using a reverse enhanced CMEA process including first and second inverse transformations and a CMEA iteration including an ehanced tbox function with inputs permuted by one or more secret offsets, the enhanced tbox function employing an involutary lookup table, the encryption/decryption processor being further operative to return the encrypted or decrypted message to the input/output interface for further routing.